格子とグラフを用いた符号の同型判定

東北大学大学院情報科学研究科

修士論文

格子とグラフを用いた
符号の同型判定

田端俊

2012年2月

目 次

1 はじめに **1**

2 Graphs and additive codes over GF(4) **1**
2.1 準備 1
2.2 Graph と GF(4) 上の additive code との関係 4
2.3 Graph による GF(4) 上の additive code の同型判定 8

3 Kleinian codes and binary codes **16**
3.1 Kleinian code から binary code への構成 16
3.2 Code の自己同型群と frame の集合の関係 17
3.2.1 Type A の frame 18
3.3 Code の自己同型群と Type B の frame の集合の関係 19
3.3.1 Length が奇数の場合 20
3.3.2 Length が偶数の場合の証明の準備 21
3.3.3 Length が偶数の場合 28
3.3.4 Code の自己同型群と Type B の frame の集合 . . . 30

4 謝辞 **30**

1 はじめに

Code とはある有限体上の有限次元線形空間である. 代数的組み合わせ論では code の分類や, グラフや格子といった他の分野との関係について主に研究されている. グラフと code との関係に関しては Danielsen-Parker[1] によって, グラフを用いての GF(4) 上の self-dual additive code の分類が行われている.

2 元体上の code からユークリッド空間の格子を構成する方法がいくつかある. 次元が 40 以上の場合 doubly even code の全ての同型類の集合と even lattice の全ての同値類の集合が 1 対 1 対応することが北詰-近藤-宮本 [3] によって示されている.

本稿では第 2 章で Danielsen-Parker[1] の Theorem 12 について別証明を与える. また, 第 3 章では Kleinian code から binary code を構成する方法と binary code の自己同型群について lattice の自己同型群と類似の命題が成り立つことを示す.

2 Graphs and additive codes over GF(4)

2.1 準備

$\mathrm{GF}(4) = \{0, 1, \omega, \omega^2\}$ を位数 4 の有限体とする. ここで $\omega^2 = \omega + 1$. $x \in \mathrm{GF}(4)$ に対して, $\overline{x} = x^2$ とする. 以下では行列は GF(4) に成分を持つものを考える. $A = (A_{ij})$ を $m \times n$ 行列とする. $\Omega_n = \{1, \ldots, n\}$ とし $S \subset \Omega_n$ とする. $\gamma_S(A)$ を

$$(\gamma_S(A))_{ij} = \begin{cases} \overline{A_{ij}} & j \in S, \\ A_{ij} & j \notin S \end{cases}$$

によって定義する. 明らかに

$$\gamma_S(\mathrm{Span}(A)) = \mathrm{Span}(\gamma_S(A)). \tag{1}$$

Lemma 1. A を $m \times n$ 行列とし, E を n 次対角行列とする. $S \subset \Omega_n$ とすると

$$\gamma_S(AE) = \gamma_S(A)\gamma_S(E)$$

が成り立つ.

Proof. $A = (A_{ij})$ とし, $E = (E_{ij})$ とする.

$$\begin{aligned}(\gamma_S(AE))_{ij} &= \begin{cases}\overline{(AE)_{ij}} & j \in S,\\ (AE)_{ij} & j \notin S\end{cases}\\ &= \begin{cases}\overline{A_{ij}}\ \overline{E_{jj}} & j \in S,\\ A_{ij}E_{jj} & j \notin S\end{cases}\\ &= \gamma_S(A)_{ij}\gamma_S(E)_{jj}\\ &= (\gamma_S(A)\gamma_S(E))_{ij}.\end{aligned}$$

□

Lemma 2. A を $m \times n$ $(0,1)$-行列とし, B を $n \times l$ 行列とする. $S \subset \Omega_n$ とすると

$$\gamma_S(AB) = A(\gamma_S(B)).$$

Proof.

$$\begin{aligned}(\gamma_S(AB))_{ij} &= \begin{cases}\overline{(AB)_{ij}} & j \in S,\\ (AB)_{ij} & j \notin S\end{cases}\\ &= \begin{cases}\overline{\sum_{k=1}^n A_{ik}B_{kj}} & j \in S,\\ \sum_{k=1}^n A_{ik}B_{kj} & j \notin S\end{cases}\\ &= \begin{cases}\sum_{k=1}^n \overline{A_{ik}B_{kj}} & j \in S,\\ \sum_{k=1}^n A_{ik}B_{kj} & j \notin S\end{cases}\\ &= \begin{cases}\sum_{k=1}^n A_{ik}\overline{B_{kj}} & j \in S,\\ \sum_{k=1}^n A_{ik}B_{kj} & j \notin S\end{cases}\\ &= (A\gamma_S(B))_{ij}.\end{aligned}$$

□

Lemma 3. A, B を $m \times n$ 行列とする. $S \subset \Omega_n$ とすると

$$\gamma_S(A + B) = \gamma_S(A) + \gamma_S(B).$$

Proof. $A = (A_{ij}), B = (B_{ij})$ とする.

$$\begin{aligned}(\gamma_S(A+B))_{ij} &= \begin{cases}\overline{A_{ij}+B_{ij}} & j \in S,\\ A_{ij}+B_{ij} & j \notin S\end{cases}\\ &= \begin{cases}\overline{A_{ij}}+\overline{B_{ij}} & j \in S,\\ A_{ij}+B_{ij} & j \notin S\end{cases} \qquad (\mathrm{GF}(4)\text{ の標数は }2)\\ &= (\gamma_S(A))_{ij} + (\gamma_S(B))_{ij}.\end{aligned}$$

□

Lemma 4. A を $m \times n$ 行列とし, $S, T \subset \Omega_n$ とする. $U = (S \cup T) \setminus (S \cap T)$ とすると

$$\gamma_U(A) = \gamma_S(\gamma_T(A)).$$

Proof. $A = (A_{ij})$ とする.

$$\begin{aligned}(\gamma_S(\gamma_T(A)))_{ij} &= \begin{cases}\overline{(\gamma_T(A))_{ij}} & j \in S,\\ (\gamma_T(A))_{ij} & j \notin S\end{cases}\\ &= \begin{cases}\overline{\overline{A_{ij}}} & j \in S \cap T,\\ \overline{A_{ij}} & j \in S \setminus T,\\ \overline{A_{ij}} & j \in T \setminus S,\\ A_{ij} & j \notin S \cup T\end{cases}\\ &= \begin{cases}\overline{A_{ij}} & j \in (S \setminus T) \cup (T \setminus S),\\ A_{ij} & \text{otherwise}\end{cases}\\ &= \begin{cases}\overline{A_{ij}} & j \in (S \cup T) \setminus (S \cap T),\\ A_{ij} & \text{otherwise}\end{cases}\\ &= \begin{cases}\overline{A_{ij}} & j \in U,\\ A_{ij} & j \notin U\end{cases}\\ &= (\gamma_U(A))_{ij}.\end{aligned}$$

□

$D : 2^{\Omega_n} \to M_n(\mathrm{GF}(2))$ を対角行列 $D(S) = (D_{ij})$ によって定義する. こ

こで

$$D_{ii} = \begin{cases} 1 & i \in S, \\ 0 & i \notin S. \end{cases} \tag{2}$$

$S = \{i\}$ のときは $D(S)$ を $D(i)$ と書く.

Lemma 5. A, B を n 次 $(0,1)$-行列とし, $S \subset \Omega_n$ とする. そのとき, $\gamma_S(A+\omega B) = A + BD(S) + \omega B$.

Proof.

$$\begin{aligned}
(\gamma_S(A+\omega B)))_{ij} &= \begin{cases} \overline{(A+\omega B)_{ij}} & j \in S, \\ (A+\omega B)_{ij} & j \notin S \end{cases} \\
&= \begin{cases} (A+\omega^2 B)_{ij} & j \in S, \\ (A+\omega B)_{ij} & j \notin S \end{cases} \\
&= \begin{cases} (A+B+\omega B)_{ij} & j \in S, \\ (A+\omega B)_{ij} & j \notin S \end{cases} \\
&= (A + BD(S) + \omega B)_{ij}.
\end{aligned}$$

□

2.2 Graph と GF(4) 上の additive code との関係

Definition 6. $\mathrm{GF}(4)^n$ の加法部分群を $\mathrm{GF}(4)$ 上の length n の additive code という.

Definition 7. $\mathcal{C}$, $\mathcal{C}'$ を length n の additive code とする. 対角行列 E, $X \subset \Omega_n$, 置換行列 P が存在して $\gamma_X(\mathcal{C}E)P = \mathcal{C}'$ となるとき 2 つの additive code は equivalent であるという.

$\boldsymbol{u} = (u_1, \ldots, u_n)$, $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathrm{GF}(4)^n$ に対して

$$\boldsymbol{u} * \boldsymbol{v} = \mathrm{Tr}(\boldsymbol{u} \cdot \overline{\boldsymbol{v}})$$

によって Hermitian trace inner product を定義する.

$\boldsymbol{a}, \boldsymbol{a}', \boldsymbol{b}, \boldsymbol{b}' \in \mathrm{GF}(2)^n$ とすると

$$\begin{aligned}
&(\boldsymbol{a} + \omega\boldsymbol{b}) * (\boldsymbol{a}' + \omega\boldsymbol{b}') \\
&= \mathrm{Tr}((\boldsymbol{a} + \omega\boldsymbol{b}) \cdot (\boldsymbol{a}' + \overline{\omega}\boldsymbol{b}')) \\
&= (\boldsymbol{a} \cdot \boldsymbol{a}') \,\mathrm{Tr}(1) + (\boldsymbol{a} \cdot \boldsymbol{b}') \,\mathrm{Tr}(\overline{\omega}) + (\boldsymbol{b} \cdot \boldsymbol{a}') \,\mathrm{Tr}(\omega) + (\boldsymbol{b} \cdot \boldsymbol{b}') \,\mathrm{Tr}(1) \\
&= (\boldsymbol{a} \cdot \boldsymbol{b}') + (\boldsymbol{b} \cdot \boldsymbol{a}').
\end{aligned}$$

Lemma 8. A, B を n 次 $(0,1)$-行列とする． GF(4) 上の additive code $\mathrm{Span}(A + \omega B)$ が self-orthogonal となる必要十分条件は

$$AB^T + BA^T = 0.$$

Proof. 上の式から $(AB^T + BA^T)_{ij}$ は $A + \omega B$ の第 i 行と第 j 行の Hermitian trace inner product に等しい．したがって $\mathrm{Span}(A + \omega B)$ が self-orthogonal である必要十分条件は $AB^T + BA^T = 0$. □

Definition 9. $\mathcal{C}$ を GF(4) 上の additive code とする．対角成分が全て 0 の対称 $(0,1)$-行列 Γ が存在して $\Gamma + \omega I$ が $\mathcal{C}$ の generator matrix となるとき $\mathcal{C}$ を graph code という．ここで I は単位行列である．Lemma 8 より graph code は self-dual additive code.

対角成分が全て 0 の n 次対称 $(0,1)$-行列 Γ に対して $N_i(\Gamma) = \{j \mid \Gamma_{ij} = 1\}$ と定義し, $M^i(\Gamma) = \{i\} \cup N_i(\Gamma)$ とおく．n 次対称 $(0,1)$-行列 Γ^i を

$$(\Gamma^i)_{kl} = \begin{cases} \Gamma_{kl} + 1 & k, l \in N_i \text{かつ } k \neq l, \\ \Gamma_{kl} & \text{otherwise} \end{cases} \tag{3}$$

によって定義する．$(\Gamma^i)^j$ を $\Gamma^{i,j}$ と表す.

Lemma 10.

$$\Gamma^i = \Gamma + D(N_i(\Gamma)) + \Gamma D(i) \Gamma.$$

Proof.

$$\begin{aligned}
(\Gamma D(i) \Gamma)_{kl} &= \Gamma_{ki} \Gamma_{il} \\
&= \begin{cases} 1 & k, l \in N_i, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned} \tag{4}$$

$$
\begin{aligned}
&(\Gamma + D(N_i(\Gamma)) + \Gamma D(i)\Gamma)_{kl} \\
&= \Gamma_{kl} + \begin{cases} 1 & k = l \in N_i, \\ 0 & \text{otherwise} \end{cases} + \begin{cases} 1 & k, l \in N_i, \\ 0 & \text{otherwise} \end{cases} \qquad ((4) \text{ より}) \\
&= \begin{cases} \Gamma_{kl} + 1 & k, l \in N_i \text{かつ } k \neq l, \\ \Gamma_{kl} & \text{otherwise} \end{cases} \\
&= (\Gamma^i)_{kl}.
\end{aligned}
$$

□

n 次対角行列 $D_k(x) = (d_{ij})$ を

$$
d_{ij} = \begin{cases} x & i = j = k, \\ 1 & i = j \neq k, \\ 0 & \text{otherwise} \end{cases}
$$

によって定義する.

$$
D_k(x) = x^2 D(k) + I \ (x = \omega, \omega^2). \tag{5}
$$

Lemma 11. Γ を対角成分が全て 0 の n 次対称 $(0,1)$-行列とする.

$$
P = \Gamma D(i) + I \tag{6}
$$

と定義する.

$$
\begin{aligned}
\Gamma^i + \omega I &= P\gamma_{M^i(\Gamma)}((\Gamma + \omega I)D_i(\omega)). \\
\mathrm{Span}(\Gamma^i + \omega I) &= \mathrm{Span}(\gamma_{M^i(\Gamma)}((\Gamma + \omega I)D_i(\omega))).
\end{aligned} \tag{7}
$$

Proof. $N_i(\Gamma)$, $M^i(\Gamma)$ をそれぞれ N_i, M^i と略記する.

$$
\begin{aligned}
(\Gamma D(i))^2 &= (\Gamma D(i)\Gamma)D(i) \\
&= O. \qquad ((4) \text{ より})
\end{aligned} \tag{8}
$$

$$
\begin{aligned}
P^2 &= (\Gamma D(i) + I)(\Gamma D(i) + I) \\
&= (\Gamma D(i))^2 + \Gamma D(i) + \Gamma D(i) + I \\
&= I. \qquad ((8) \text{ より})
\end{aligned}
$$

よって $P \in \mathrm{GL}(n,2)$ で $P^{-1} = P$.

$$
\begin{aligned}
&P\gamma_{M^i}((\Gamma+\omega I)D_i(\omega)) \\
&= \gamma_{M^i}(P(\Gamma+\omega I)D_i(\omega)) && \text{(Lemma 2 より)} \\
&= \gamma_{M^i}(P(\Gamma+\omega I)(\omega^2 D(i)+I)) && \text{((5) より)} \\
&= \gamma_{M^i}(P(\omega^2\Gamma D(i)+\Gamma+D(i)+\omega I)) \\
&= \gamma_{M^i}(P(\Gamma D(i)+\Gamma+D(i))+\omega P(\Gamma D(i)+I)) \\
&= \gamma_{M^i}(P(\Gamma D(i)+\Gamma+D(i))+\omega I) && \text{((6) より)} \\
&= P(\Gamma D(i)+\Gamma+D(i))+D(M^i)+\omega I && \text{(Lemma 5 より)} \\
&= (\Gamma D(i)+I)(\Gamma D(i)+\Gamma+D(i))+D(M^i)+\omega I && \text{((6) より)} \\
&= (\Gamma D(i))^2+\Gamma D(i)\Gamma+\Gamma D(i)^2+\Gamma D(i)+\Gamma+D(i) \\
&\quad +D(M^i)+\omega I \\
&= (\Gamma D(i))^2+\Gamma D(i)\Gamma+\Gamma+D(N^i)+\omega I \\
&= \Gamma+D(N_i)+\Gamma D(i)\Gamma+\omega I && \text{((8) より)} \\
&= \Gamma^i+\omega I. && \text{(Lemma 10 より)}
\end{aligned}
$$

P を左から掛けることは行基本変形に対応するので span は不変. したがって (7) を得る. □

Lemma 12. $v_1,\ldots,v_l \in \Omega_n$ とすると $\mathrm{Span}(\Gamma+\omega I)$ と $\mathrm{Span}(\Gamma^{v_1,\ldots,v_l}+\omega I)$ は equivalent.

Proof. l に関する帰納法によって示す. $l=1$ のときは (7) から成り立つ.

$\Gamma' = \Gamma^{v_1,\ldots,v_{l-1}}$ とおき $\mathrm{Span}(\Gamma+\omega I)$ と $\mathrm{Span}(\Gamma'+\omega I)$ が equivalent とすると (7) から

$$\mathrm{Span}((\Gamma')^{v_l}+\omega I) = \mathrm{Span}(\gamma_{M^i(\Gamma')}((\Gamma'+\omega I)D_i(\omega))).$$

右辺は $\mathrm{Span}(\Gamma'+\omega I)$ と equivalent なので $\mathrm{Span}(\Gamma+\omega I)$ とも equivalent である. □

Lemma 13. A, B を n 次 $(0,1)$-行列とする. $\mathrm{GF}(4)$ 上の self-dual additive code $\mathrm{Span}(A+\omega B)$ が graph code となる必要十分条件は B が正則でかつ任意の $i \in \Omega_n$ に対して $(B^{-1}A)_{ii} = 0$ となることである.

Proof. $\mathrm{Span}(A+\omega B)$ が graph code とすると任意の $i \in \Omega_n$ に対して $(XA)_{ii} = 0$, かつ $XB = I$ を満たすような正則行列 X が存在する. $X =$

B^{-1} である. 逆に B が正則とすると,

$$\mathrm{Span}(A+\omega B) = \mathrm{Span}(B^{-1}A+\omega I).$$

Lemma 8 より $(B^{-1}A)I^T + I(B^{-1}A)^T = O$. よって $(B^{-1}A)^T = B^{-1}A$ が成り立つ. また, 任意の $i \in \Omega_n$ に対して $(B^{-1}A)_{ii} = 0$ であるから $\mathrm{Span}(A+\omega B)$ は graph code である. □

2.3 Graph による GF(4) 上の additive code の同型判定

Lemma 14. $\Gamma, \Gamma' \in M_n(\mathrm{GF}(2))$ とする. もし $\mathrm{Span}(\Gamma+\omega I) = \mathrm{Span}(\Gamma'+\omega I)$ なら, $\Gamma = \Gamma'$.

Proof. $i \in \Omega_n$ とする. そのとき, $u \in \mathrm{GF}(2)^n$ が存在して

$$(\Gamma'+\omega I \text{ の第 } i \text{ 行}) = u(\Gamma+\omega I) \tag{9}$$

となる. $j \in \Omega_n$ に対して,

$$\begin{aligned} j \neq i &\iff (\Gamma'+\omega I)_{ij} \in \mathrm{GF}(2) \\ &\iff (u(\Gamma+\omega I))_j \in \mathrm{GF}(2) \qquad ((9) \text{ より}) \\ &\iff \omega u_j \in \mathrm{GF}(2) \\ &\iff u_j = 0. \end{aligned}$$

よって u は第 i 成分が 1 の単位ベクトルで $u(\Gamma+\omega I)$ は $\Gamma+\omega I$ の第 i 行である. (9) からこれは $\Gamma'+\omega I$ の第 i 行に等しい. 任意の $i \in \Omega_n$ に対して, これが成り立つので $\Gamma'+\omega I = \Gamma+\omega I$. したがって $\Gamma' = \Gamma$. □

対角行列 $E = (E_{ij})$ に対して, $\mathrm{supp}(E) = \{i \mid E_{ii} \neq 0\}$ と定義する.

$$E = E_0 + \omega E_1 + \omega^2 E_2 \tag{10}$$

を正則な対角行列とする. ここで E_0, E_1, E_2 は $(0,1)$-対角行列で任意の $i, j \in \{0,1,2\}$, $i \neq j$ に対して

$$\mathrm{supp}(E_i) \cap \mathrm{supp}(E_j) = \emptyset. \tag{11}$$

$X_j(E) = \{i \mid (E_j)_{ii} \neq 0\}$ とし, $L(E) = X_1(E) \cup X_2(E)$ とする. 対角成分が全て 0 の n 次対称 $(0,1)$-行列 Γ に対して

$$\mathcal{E}(\Gamma) := \{E \mid E \text{ は正則な対角行列でかつ} \Gamma(E_1+E_2)+E_0+E_1 \text{が正則 }\}.$$

$$S_\Gamma : \mathcal{E}(\Gamma) \to 2^{\Omega_n}$$

を

$$S_\Gamma(E) = \{i \mid ((\Gamma(E_1+E_2)+E_0+E_1)^{-1}(\Gamma(E_0+E_2)+E_1+E_2))_{ii} = 1\} \quad (12)$$

によって定義する.

Lemma 15. $E \in \mathcal{E}(\Gamma)$, $S \subset \Omega_n$ とし, $\mathcal{C} = \mathrm{Span}(\gamma_S((\Gamma + \omega I)E))$ とする. そのとき, $\mathcal{C}$ が graph code となる必要十分条件は $E \in \mathcal{E}(\Gamma)$ で

$$S = S_\Gamma(E)$$

が成り立つことである.

Proof.

$$\begin{aligned}
&(\Gamma + \omega I)E \\
&= (\Gamma + \omega I)(E_0 + \omega E_1 + \omega^2 E_2) \\
&= \Gamma(E_0 + \omega E_1 + \omega^2 E_2) + \omega(E_0 + \omega E_1 + \omega^2 E_2) \\
&= \Gamma(E_0 + E_2) + E_1 + E_2 + \omega(\Gamma(E_1 + E_2) + E_0 + E_1).
\end{aligned}$$

ここで

$$\begin{aligned}
A &= \Gamma(E_0 + E_2) + E_1 + E_2, \\
B &= \Gamma(E_1 + E_2) + E_0 + E_1
\end{aligned}$$

とおくと Lemma 5 から $\mathcal{C} = \mathrm{Span}(A + BD(S) + \omega B)$. Lemma 13 より $\mathcal{C}$ が graph code である必要十分条件は B が正則かつ任意の $i \in \Omega_n$ に対して $(B^{-1}(A + BD(S)))_{ii} = 0$ となることである. $(B^{-1}(A + BD(S)))_{ii} = 0$ となる必要十分条件は $(B^{-1}A)_{ii} = 1$ と $(D(S))_{ii} = 1$ が同値となることである. よって

$$\begin{aligned}
S &= \{i \mid (D(S))_{ii} = 1\} \\
&= \{i \mid (B^{-1}A)_{ii} = 1\} \\
&= S_\Gamma(E).
\end{aligned}$$

□

Γ を固定し, 以後 $\mathcal{E}_\Gamma$ を $\mathcal{E}$, S_Γ を S と書く.

$$E^i := \begin{cases} ED_i(\omega^2) & i \in S(E), \\ ED_i(\omega) & i \notin S(E) \end{cases} \tag{13}$$

Lemma 16. $E \in \mathcal{E}$ とし,

$$\mathrm{Span}(\gamma_{S(E)}((\Gamma + \omega I)E)) = \mathrm{Span}(\Gamma' + \omega I) \tag{14}$$

が成り立つとする. $E^i \in \mathcal{E}$ で

$$S(E^i) = (M^i(\Gamma') \cup S(E)) \setminus (M^i(\Gamma') \cap S(E)). \tag{15}$$

$$\mathrm{Span}(\gamma_{S(E^i)}((\Gamma + \omega I)E^i)) = \mathrm{Span}((\Gamma')^i + \omega I). \tag{16}$$

Proof. $M^i(\Gamma')$ を M^i と書く. $X = (M^i \cup S(E)) \setminus (M^i \cap S(E))$ とおく. $i \in M^i$ であるから

$$i \in S(E) \text{ ならば } i \notin X, \tag{17}$$

$$i \notin S(E) \text{ ならば } i \in X. \tag{18}$$

$$\begin{aligned} \gamma_X(E^i) &= \begin{cases} \gamma_X(ED_i(\omega^2)) & i \in S(E), \\ \gamma_X(ED_i(\omega)) & i \notin S(E) \end{cases} && ((13) \text{ より}) \\ &= \begin{cases} \gamma_X(E)\gamma_X(D_i(\omega^2)) & i \in S(E), \\ \gamma_X(E)\gamma_X(D_i(\omega)) & i \notin S(E) \end{cases} && (\text{Lemma 1 より}) \\ &= \begin{cases} \gamma_X(E)\gamma_X(D_i(\omega^2)) & i \notin X, \\ \gamma_X(E)\gamma_X(D_i(\omega)) & i \in X \end{cases} && ((17), (18) \text{ より}) \\ &= \gamma_X(E)D_i(\omega^2). && (19) \end{aligned}$$

$$\begin{aligned} \gamma_X((\Gamma + \omega I)E^i) &= \gamma_X(\Gamma + \omega I)\gamma_X(E^i) && (\text{Lemma 1 より}) \\ &= \gamma_X((\Gamma + \omega I)E)D_i(\omega^2). && ((19) \text{ より}) \quad (20) \end{aligned}$$

$i \in M^i$ より

$$\gamma_{M^i}(D_i(\omega)) = D_i(\omega^2) \tag{21}$$

$$
\begin{aligned}
&\mathrm{Span}(\gamma_X((\Gamma+\omega I)E^i)) \\
&= \mathrm{Span}(\gamma_X((\Gamma+\omega I)E)D_i(\omega^2)) && ((20)\text{ より}) \\
&= \mathrm{Span}((\gamma_{M^i}(\gamma_{S(E)}((\Gamma+\omega I)E)))D_i(\omega^2)) && (\text{Lemma 4 より}) \\
&= \mathrm{Span}(\gamma_{M^i}(\gamma_{S(E)}((\Gamma+\omega I)E))\gamma_{M^i}(D_i(\omega))) && ((21)\text{ より}) \\
&= \mathrm{Span}(\gamma_{M^i}(\gamma_{S(E)}(\Gamma+\omega I)E))\gamma_{M^i}(D_i(\omega)) \\
&= \gamma_{M^i}(\mathrm{Span}(\gamma_{S(E)}(\Gamma+\omega I)E))\gamma_{M^i}(D_i(\omega)) && ((1)\text{ より}) \\
&= \gamma_{M^i}(\mathrm{Span}(\Gamma'+\omega I))\gamma_{M^i}(D_i(\omega)) && ((14)\text{ より}) \\
&= \mathrm{Span}(\gamma_{M^i}((\Gamma'+\omega I)D_i(\omega))) && ((1)\text{ より}) \\
&= \mathrm{Span}((\Gamma')^i+\omega I). && ((7)\text{ より})
\end{aligned}
$$

よって $\mathrm{Span}(\gamma_X((\Gamma+\omega I)E^i))$ は graph code となる. したがって Lemma 15 から $E^i \in \mathcal{E}$ であり $X = S(E^i)$. □

Lemma 17. $E \in \mathcal{E}$ とし, (14) が成り立つとする. $(v_1, \ldots, v_i)$ を Ω_n に値を持つ列とする. そのとき $E^{v_1,\ldots,v_l} \in \mathcal{E}$ であり,

$$\mathrm{Span}((\Gamma')^{v_1,\ldots,v_l}+\omega I) = \mathrm{Span}(\gamma_{S(E^{v_1,\ldots,v_l})}((\Gamma+\omega I)E^{v_1,\ldots,v_l})) \tag{22}$$

Proof. l に関する帰納法によって示す. $l = 1$ のときは Lemma 16 の (16) によって成り立つ.

$\Gamma'' = (\Gamma')^{v_1,\ldots,v_{l-1}}$ とおく. $M^{v_l}(\Gamma'')$ を M, $E^{v_1,\ldots,v_{l-1}}$ を E'' と略記する.

$$\mathrm{Span}(\Gamma''+\omega I) = \mathrm{Span}(\gamma_{S(E'')}((\Gamma+\omega I)E'')) \tag{23}$$

が成り立つとする. $v_l \in M$ より

$$\gamma_M(D_{v_l}(\omega)) = D_{v_l}(\omega^2). \tag{24}$$

Lemma 16 より $(E'')^{v_l} \in \mathcal{E}$ であり, (15) より

$$S((E'')^{v_l}) = (M \cup S(E'')) \setminus (M \cap S(E'')). \tag{25}$$

$$
\begin{aligned}
&\mathrm{Span}((\Gamma')^{v_1,\dots,v_l}+\omega I)\\
&=\mathrm{Span}((\Gamma'')^{v_l}+\omega I)\\
&=\mathrm{Span}(\gamma_M((\Gamma''+\omega I)D_{v_l}(\omega))) && ((7)\text{ より})\\
&=\mathrm{Span}(\gamma_M(\Gamma''+\omega I)\gamma_M(D_{v_l}(\omega))) && (\text{Lemma 1 より})\\
&=\mathrm{Span}(\gamma_M(\Gamma''+\omega I))\gamma_M(D_{v_l}(\omega))\\
&=\gamma_M(\mathrm{Span}(\Gamma''+\omega I))\gamma_M(D_{v_l}(\omega)) && ((1)\text{ より})\\
&=\gamma_M(\mathrm{Span}(\gamma_{S(E'')}((\Gamma+\omega I)E'')))\gamma_M(D_{v_l}(\omega)) && ((23)\text{ より})\\
&=\mathrm{Span}(\gamma_M(\gamma_{S(E'')}((\Gamma+\omega I)E''))\gamma_M(D_{v_l}(\omega))) && ((1)\text{ より})\\
&=\mathrm{Span}(\gamma_M(\gamma_{S(E'')}((\Gamma+\omega I)E''))D_{v_l}(\omega^2)) && ((24)\text{ より})\\
&=\mathrm{Span}(\gamma_{(M\cup S(E''))\setminus(M\cap S(E''))}((\Gamma+\omega I)E'')D_{v_l}(\omega^2)) && (\text{Lemma 4 より})\\
&=\mathrm{Span}(\gamma_{S((E'')^{v_l})}((\Gamma+\omega I)E'')D_{v_l}(\omega^2)) && ((25)\text{ より})\\
&=\mathrm{Span}(\gamma_{S((E'')^{v_l})}((\Gamma+\omega I)(E'')^{v_l})). && ((20)\text{ より})
\end{aligned}
$$

□

Lemma 18. $E\in\mathcal{E}$, $E\neq I$ とし, (14) が成り立つとする. 次のいずれかが成り立つ.

(i) $X_1(E)\cap S(E)\neq\emptyset$

(ii) $X_2(E)\setminus S(E)\neq\emptyset$

(iii) ある $i,j\in L(E)$ が存在して $\Gamma'_{ij}=1$

Proof. (i), (ii), (iii) のいずれも成り立たないとする. (i) が成り立たないことから任意の $x\in\mathrm{GF}(4)$ に対して

$$\gamma_{S(E)}(xE_1)=xE_1. \tag{26}$$

また (ii) が成り立たないことから, 任意の $x\in\mathrm{GF}(4)$ に対して

$$.\gamma_{S(E)}(xE_2)=\overline{x}E_2 \tag{27}$$

$E'=E_0+\omega^2(E_1+E_2)$ とすると

$$
\begin{aligned}
&E\gamma_{S(E)}(E')=E\gamma_{S(E)}(E_0+\omega^2(E_1+E_2))\\
&=E(\gamma_{S(E)}(E_0)+\gamma_{S(E)}(\omega^2E_1)+\gamma_{S(E)}(\omega^2E_2)) && (\text{Lemma 3 より})\\
&=E(E_0+\omega^2E_1+\omega E_2) && ((26),\ (27)\text{ より})\\
&=(E_0+\omega E_1+\omega^2E_2)(E_0+\omega^2E_1+\omega E_2) && ((10)\text{ より})\\
&=I && ((11)\text{ より}) \qquad (28)
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{Span}(\gamma_{S(E)}((\Gamma'+\omega I)E')) \\
&= \mathrm{Span}(\gamma_{S(E)}(\Gamma'+\omega I)\gamma_{S(E)}(E')) && \text{(Lemma 1 より)} \\
&= \mathrm{Span}(\gamma_{S(E)}(\Gamma'+\omega I))\gamma_{S(E)}(E') \\
&= \mathrm{Span}((\Gamma+\omega I)E)\gamma_{S(E)}(E') && \text{((14) より)} \\
&= \mathrm{Span}((\Gamma+\omega I)E\gamma_{S(E)}(E')) \\
&= \mathrm{Span}(\Gamma+\omega I) && \text{((28) より)}
\end{aligned}
$$

となるので、$\mathrm{Span}(\gamma_{S(E)}((\Gamma'+\omega I)E'))$ は graph code である. したがって Lemma 15 より $E' \in \mathcal{E}(\Gamma')$, すなわち $\Gamma'(E_1+E_2)+E_0$ は正則とならなければならない. 一方 (iii) が成り立たないことから

$$
\begin{aligned}
\Gamma'(E_1+E_2)+E_0 &= \begin{pmatrix} & X_0(E) & L(E) \\ & & \\ & O & \end{pmatrix} \begin{pmatrix} O & O \\ O & I \end{pmatrix} + \begin{pmatrix} I & O \\ O & O \end{pmatrix} \\
&= \begin{pmatrix} O & O \end{pmatrix}
\end{aligned}
$$

これは $\Gamma'(E_1+E_2)+E_0$ が正則となることに矛盾. □

Lemma 19. $E \in \mathcal{E}$ とし, (14) が成り立つとする. Ω_n に値を持つ列 $(v_1, \ldots, v_l)$ が存在して $(\Gamma')^{v_1,\ldots,v_l} = \Gamma$ となる.

Proof. $|L(E)|$ に関する帰納法で示す. $|L(E)| = 0$ のとき $E = I$. よって $E = E_0$ であるから

$$
\begin{aligned}
S(E) &= \{i \mid (E_0^{-1}\Gamma E_0)_{ii} = 1\} && \text{((12) より)} \\
&= \{i \mid \Gamma_{ii} = 1\} \\
&= \emptyset.
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{Span}(\Gamma'+\omega I) &= \mathrm{Span}(\gamma_{S(E)}((\Gamma+\omega I)E)) && \text{((14) より)} \\
&= \mathrm{Span}(\gamma_{\emptyset}((\Gamma+\omega I)I)) \\
&= \mathrm{Span}(\Gamma+\omega I).
\end{aligned}
$$

よって Lemma 14 から $\Gamma' = \Gamma$.

$|L(E)| \leq k$ のとき Lemma が成り立つと仮定する. $|L(E)| = k+1$ のとき $E \neq I$ であるから Lemma 18 の (i), (ii), (iii) の条件のいずれかを満たす.

(i) $i \in X_1(E) \cap S(E)$ とすると $|L(E^i)| = |L(E)| - 1$.

(ii) $i \in X_2(E) \setminus S(E)$ とすると $|L(E^i)| = |L(E)| - 1$.

(iii) $\exists i, j \in (X_1(E) \setminus S(E)) \cup (X_2(E) \cap S(E))$ s.t. $\Gamma'_{ij} = 1$.

(iii) のとき $j \in M^i(\Gamma')$ だから (15) から

$$j \in S(E) \text{ のとき}, j \notin S(E^i). \tag{29}$$
$$j \notin S(E) \text{ のとき}, j \in S(E^i). \tag{30}$$

(iii)-(1) $i, j \in X_1(E) \setminus S(E)$ のとき

$$E^i = ED_i(\omega).$$

(30) より $j \in S(E^i)$. (13) より

$$E^{i,j} = ED_i(\omega)D_j(\omega^2).$$

$$|X_1(E^{i,j})| = |X_1(E) \setminus \{i, j\}| = |X_1(E)| - 2,$$
$$|X_2(E^{i,j})| = |X_2(E) \cup \{i\}| = |X_2(E)| + 1.$$

(iii)-(2) $i \in X_1 \setminus S(E)$, $j \in X_2 \cap S(E)$ のとき

$$(E^i)^j = ED_i(\omega)D_j(\omega).$$

$$|X_1(E^{i,j})| = |X_1(E) \setminus \{i\}| = |X_1(E)| - 1,$$
$$|X_2(E^{i,j})| = |X_2(E) \cup \{i\} \setminus \{j\}| = |X_2(E)|.$$

(iii)-(3) $i, j \in X_2 \cap S(E)$ のとき

$$(E^i)^j = ED_i(\omega^2)D_j(\omega).$$

$$|X_1(E^{i,j})| = |X_1(E) \cup \{i\}| = |X_1(E)| + 1,$$
$$|X_2(E^{i,j})| = |X_2(E) \setminus \{i, j\}| = |X_2(E)| - 2.$$

いずれの場合も $|L(E^{i,j})| = |L(E)| - 1$.

以上より $|L(E^i)| = |L(E)| - 1$ となるような $i \in \Omega_n$ が存在するか, または, $|L(E^{i,j})| = |L(E)| - 1$ となるような $i, j \in \Omega_n$ が存在する. 前者の場合 (22) より

$$\mathrm{Span}((\Gamma')^i + \omega I) = \mathrm{Span}(\gamma_{S(E^i)}((\Gamma + \omega I)E^i)).$$

よって帰納法の仮定から Ω_n に値を持つ列 $(v_1, \ldots, v_l)$ が存在して

$$(\Gamma')^{i,v_1 \ldots, v_l} = \Gamma.$$

$|L(E^{i,j})| = |L(E)| - 1$ となるような $i, j \in \Omega_n$ が存在する場合も同様. □

Theorem 20. $\mathcal{C} = \mathrm{Span}(\Gamma + \omega I)$, $\mathcal{C}' = \mathrm{Span}(\Gamma' + \omega I)$ を graph code とする. $\mathcal{C}, \mathcal{C}'$ が equivalent となる必要十分条件は列 $(v_1, \ldots, v_i)$ が存在してある置換行列 P に対して $\Gamma = (P\Gamma' P^T)^{v_1, \ldots, v_i}$ となることである.

Proof.

$\mathcal{C}$ と$\mathcal{C}'$が equivalent
$\iff \exists E$: 対角行列, $\exists X \subset \Omega_n, \exists P$: 置換行列,
$\gamma_X(\mathrm{Span}(\Gamma + \omega I)E)P = \mathrm{Span}(\Gamma' + \omega I)$
$\iff \exists E$: 対角行列, $\exists X \subset \Omega_n, \exists P$: 置換行列,
$\mathrm{Span}(\gamma_X((\Gamma + \omega I)E))P = \mathrm{Span}(\Gamma' + \omega I)$ ((1) より)
$\iff \exists E$: 対角行列, $\exists X \subset \Omega_n, \exists P$: 置換行列,
$\mathrm{Span}(\gamma_X((\Gamma + \omega I)E)) = \mathrm{Span}(\Gamma' + \omega I)P^T$
$\iff \exists E$: 対角行列, $\exists X \subset \Omega_n, \exists P$: 置換行列,
$\mathrm{Span}(\gamma_X((\Gamma + \omega I)E)) = \mathrm{Span}(P\Gamma' P^T + \omega I)$
$\iff \exists E$: 対角行列, $\exists P$: 置換行列,
$\mathrm{Span}(\gamma_{S(E)}((\Gamma + \omega I)E)) = \mathrm{Span}(P\Gamma' P^T + \omega I)$ (Lemma 15 より)
$\implies \exists P$: 置換行列, $\exists (v_1, \ldots, v_l), (P\Gamma P^T)^{v_1, \ldots, v_l} = \Gamma$ (Lemma 19 より)

逆に $(v_1, \ldots, v_i)$ が存在してある置換行列 P に対して $\Gamma = (P\Gamma' P^T)^{v_1, \ldots, v_i}$ が成り立つとする.

Lemma 12 より $\mathrm{Span}((P\Gamma' P^T)^{v_1, \ldots, v_i} + \omega I)$ と $\mathrm{Span}(P\Gamma' P^T + \omega I)$ は equivalent. また $\mathrm{Span}(P\Gamma' P^T + \omega I)$ と $\mathrm{Span}(\Gamma' + \omega I)$ が equivalent であることから $\mathrm{Span}(\Gamma + \omega I)$ と $\mathrm{Span}(\Gamma' + \omega I)$ は equivalent である. □

3 Kleinian codes and binary codes

3.1 Kleinian code から binary code への構成

$K = \{0, a, b, c\}$ をクライン群とする. ここで 0 は単位元であり, $a + b = c, 2a = 2b = 0$ である. $\mathcal{C} \subset K^n$ を K 上の length n の code という. $\mathcal{C}$ が K^n の部分群であるとき linear であるという.

$\boldsymbol{F}_2 = \{0, 1\}$ を位数 2 の有限体とする. ここで 0 は零元であり, 1 は単位元である. $\mathcal{D} \subset \boldsymbol{F}_2^n$ を $\boldsymbol{F}_2$ 上の length n の code という. また, $\mathcal{D}$ が $\boldsymbol{F}_2^n$ の部分群であるとき linear であるという. $\boldsymbol{F}_2^n$ の内積を $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \boldsymbol{F}_2^n$ に対して $x \cdot y = \sum_{i=1}^n x_i y_i$ と定義する.

また, $x = (x_1, x_2), y = (y_1, y_2) \in \boldsymbol{F}_2^2$ に対して $(x, y) = x_1 y_2 + x_2 y_1$ とすると $(,)$ は $\boldsymbol{F}_2^2$ の内積である.

$$\mathcal{D}^\perp = \{x \in F_2^n \mid \text{任意の } y \in \mathcal{C} \text{ に対して } x \cdot y = 0\}$$

を $\mathcal{D}$ の dual code という. $\mathcal{D} \subset \mathcal{D}^\perp$ のとき $\mathcal{D}$ は self-orthogonal であるという. $\hat{}: K \to \boldsymbol{F}_2^4$ を $\hat{0} = (0000)$, $\hat{a} = (1100)$, $\hat{b} = (1010)$, $\hat{c} = (0110)$ によって定義する. また, $\widehat{}: K^n \to \boldsymbol{F}_2^{4n}$ を

$$\widehat{x} = (\hat{x_1}, \ldots, \hat{x_n})$$

によって定義する. $D_4^n = \{(0000), (1111)\}^n$ とする.

Lemma 21. $(D_4^n)^\perp = \bigcup_{x \in K^n} (D_4^n + \widehat{x})$.

Proof. $D_4^n \subset (D_4^n)^\perp$, $\widehat{K^n} \subset (D_4^n)^\perp$ より $(D_4^n)^\perp \supset \bigcup_{x \in K^n} (D_4^n + \widehat{x})$.

$$|(D_4^n)^\perp| = 2^{3n} = \left| \bigcup_{x \in K^n} (D_4^n + \widehat{x}) \right|.$$

□

Lemma 22. $\mathcal{D}$ を self-orthogonal binary code とし, $D_4^n \subset \mathcal{D}$ とする. $\mathcal{C} = \{x \in K^n \mid (D_4^n + \widehat{x}) \cap \mathcal{D} \neq \emptyset\}$ とすると $\mathcal{D} = D_4^n + \widehat{\mathcal{C}}$.

Proof. $D_4^n \subset \mathcal{D}$ より $x \in K^n$ に対して

$$(D_4^n + \widehat{x}) \cap \mathcal{D} \neq \emptyset \iff D_4^n + \widehat{x} \subset \mathcal{D}. \tag{31}$$

$$
\begin{aligned}
\mathcal{D} &= \mathcal{D} \cap (D_4^n)^\perp \\
&= \mathcal{D} \cap \left(\bigcup_{x \in K^n} (D_4^n + \widehat{x}) \right) && \text{(Lemma 21 より)} \\
&= \bigcup_{x \in K^n} ((D_4^n + \widehat{x}) \cap \mathcal{D}) \\
&= \bigcup_{x \in \mathcal{C}} ((D_4^n + \widehat{x}) \cap \mathcal{D}) \\
&= \bigcup_{x \in \mathcal{C}} (D_4^n + \widehat{x}) && \text{((31) より)} \\
&= D_4^n + \widehat{\mathcal{C}}.
\end{aligned}
$$

□

3.2 Code の自己同型群と frame の集合の関係

自然数 n に対して $\Omega_n = \{1, \ldots, n\}$ とする． $\mathcal{D}$ を length $4n$ の self-orthogonal binary code とする． $\{e_1, \ldots, e_n\} \subset \boldsymbol{F}_2^{4n}$ が次の条件を満たすとき $\mathcal{D}$ の frame という．

- 任意の $i, j \in \Omega_n$ に対して $e_i + e_j \in \mathcal{D}$.
- 任意の $i \in \Omega_n$ に対して $\mathrm{wt}(e_i) = 4$.
- $i \neq j$ となる $i, j \in \Omega_n$ に対して $\mathrm{supp}(e_i) \cap \mathrm{supp}(e_j) = \emptyset$.

$X \subset \Omega_{4n}$, $e_X \in \boldsymbol{F}_2^{4n}$ を

$$
(e_X)_i = \begin{cases} 1 & (i \in X), \\ 0 & (i \notin X) \end{cases}
$$

によって定義する．$X = \{x\}$ のときは e_X を e_x と書く．

Lemma 23. $\mathcal{F}$ を $\mathcal{D}$ の frame の集合で次の条件を満たすものとする．$E \in \mathcal{F}$ を固定する．任意の $F \in \mathcal{F} \setminus \{E\}$ に対して $|F \cap E| < |\tau(F) \cap E|$ を満たす $\tau \in \mathrm{Aut}(\mathcal{D})$ が存在するものとする．そのとき任意の $F \in \mathcal{F}$ に対して $\sigma(F) = E$ を満たす $\sigma \in \mathrm{Aut}(\mathcal{D})$ が存在する．

Proof. $F \in \mathcal{F}$ とする. $n - |F \cap E|$ に関する帰納法によって示す. $F = E$ のときは単位置換 $e \in \mathrm{Aut}(\mathcal{D})$ によって $e(F) = E$. $|F \cap E| \geq k$ となる任意の $F \in \mathcal{F}$ に対して $\rho \in \mathrm{Aut}(\mathcal{D})$ が存在して $\rho(F) = E$ とする. $F' \in \mathcal{F}$ とし $|F' \cap E| = k-1$ とする. $\tau \in \mathrm{Aut}(\mathcal{D})$ が存在して $|F' \cap E| < |\tau(F') \cap E|$. $|\tau(F') \cap E| \geq k$ より $\rho \in \mathrm{Aut}(\mathcal{D})$ が存在して $\rho\tau(F') = E$. □

Lemma 24. $\mathcal{D}$ を self-orthogonal binary code とし, $\mathrm{wt}(x) = 4$ となる $x \in \mathcal{D}$ が存在すると仮定する. $\mathrm{supp}(x) = \{i, j, k, l\}$ とすると $(i, j)(k, l) \in \mathrm{Aut}(\mathcal{D})$.

Proof. $y \in \mathcal{D}$ とする. $\mathrm{wt}((y_i, y_j, y_k, y_l)) \equiv 0 \pmod 4$ のとき $(i, j)(k, l)y = y$. $\mathrm{wt}((y_i, y_j, y_k, y_l)) = 2$ のとき

$$(y_i, y_j, y_k, y_l) \in \{(1100), (0011), (1010), (0101), (1001), (0110)\}.$$

$y_i = y_j$ のとき $(i, j)(k, l)y = y$. $y_i \neq y_j$ のとき $(i, j)(k, l)y = y + x$. よって任意の $y \in \mathcal{D}$ に対して $(i, j)(k, l)y \in \mathcal{D}$. □

Definition 25. $i \in \Omega_n$ に対して $I_i = \{4i - 3, 4i - 2, 4i - 1, 4i\}$ とする. $F_0 = \{e_{I_1}, \ldots, e_{I_n}\}$ とする. $\mathcal{D}$ の frame F が $F \subset \mathcal{D}$ をみたすとき F は Type A であるという. F が Type A ではないが $F \subset \mathcal{D}^{\perp}$ を満たすとき F を Type B と呼ぶ.

$D_4^n = \sum_{f \in F_0} \boldsymbol{F}_2 f$ である.

3.2.1 Type A の frame

Lemma 26. $\mathcal{D}$ を F_0 を frame として持つ self-orthogonal binary code とし, F_0 を Type A とする. そのとき, $F \neq F_0$ である $\mathcal{D}$ の Type A の任意の frame F に対して $|F \cap F_0| < |\sigma(F) \cap F_0|$ を満たす $\sigma \in \mathrm{Aut}(\mathcal{D})$ が存在する.

Proof. 任意の $f \in F \setminus (F_0 \cap F)$ に対して $i \neq j$ となる $i, j \in \Omega_n$ と $X_k \subset I_k$, $|X_k| = 2$ $(k = i, j)$ が存在して

$$f = e_{X_i} + e_{X_j}.$$

$\{s, t\} = X_i, \{u, r\} = I_j \setminus X_j$ とし $\sigma = (s, u)(t, r)$ とすると

$$\sigma(f) = e_{I_j}.$$

$f + e_{I_j} \in \mathcal{D}$ で $\mathrm{supp}(f + e_{I_j}) = \{s, t, u, r\}$. Lemma 24 より $\sigma \in \mathrm{Aut}(\mathcal{D})$. また $e_{I_i}, e_{I_j} \notin F$. 任意の $e \in F_0 \setminus \{e_{I_i}, e_{I_j}\}$ に対して $\sigma(e) = e$. よって $|F \cap F_0| < |\sigma(F) \cap F_0|$. □

Theorem 27. n を自然数とする. $\mathcal{D}$ を Type A の frame を少なくとも 1 つは持つ length $4n$ の self-orthogonal binary code とする. そのとき $\mathrm{Aut}(\mathcal{D})$ は全ての Type A の frame の集合上 transitive.

Proof. $\mathcal{D}$ は F_0 を Type A の frame として持つと仮定しても一般性を失わない. $\mathcal{F}$ を $\mathcal{D}$ の Type A の frame 全体の集合とする. Lemma 26 から任意の $F \in \mathcal{F} \setminus \{F_0\}$ に対して $|F \cap F_0| < |\sigma(F) \cap F_0|$ である. Lemma 23 より $\mathrm{Aut}(\mathcal{D})$ は $\mathcal{F}$ 上 transitive である. □

3.3 Code の自己同型群と Type B の frame の集合の関係

Lemma 28. $\mathcal{D}$ を length $4n$ の self-orthogonal binary code とし, F_0 を Type B の frame として持つとする. F を $\mathcal{D}$ の Type B の frame で $F \neq F_0$ かつ $F \cap F_0 \neq \emptyset$ とすると $|F \cap F_0| < |\sigma(F) \cap F_0|$ を満たす $\sigma \in \mathrm{Aut}(\mathcal{D})$ が存在する.

Proof. $k \in \Omega_n$ が存在して $e_{I_k} \in F \cap F_0$. 任意の $f \in F \setminus (F \cap F_0)$ に対して

$$f + e_{I_k} \in \mathcal{D} \subset (d_4^n)^\perp.$$

よって $f \in (d_4^n)^\perp$. $\mathrm{wt}(f) = 4$ であるから $i \neq j$ となる $i, j \in \Omega_n$ が存在して

$$f = e_{X_i} + e_{X_j}.$$

ここで $X_l \subset I_l$, $|X_l| = 2$ $(l = i, j)$. $\{s, t\} = X_i, \{u, r\} = I_j \setminus X_j$ とし, $\sigma = (s, u)(t, r)$ とすると

$$\sigma(f) = e_{I_j}.$$

任意の $e \in F_0 \setminus \{e_{I_i}, e_{I_j}\}$ に対して $\sigma(e) = e$. また $e_{I_i}, e_{I_j} \notin F$. ここで

$$\begin{aligned} e_{X_i} + e_{I_j \setminus X_j} &= f + e_{I_k} + e_{I_k} + e_{I_j} \\ &\in \mathcal{D}. \end{aligned}$$

Lemma 24 より $\sigma \in \mathrm{Aut}(\mathcal{D})$. よって $|F \cap F_0| < |\sigma(F) \cap F_0|$. □

Lemma 29. $n \geq 5$ とする. $\mathcal{D}$ を length $4n$ の self-orthogonal binary code とし, F_0 を Type B の frame として持つとする. F を $\mathcal{D}$ の Type B の frame で $F \cap F_0 = \emptyset$ とすると任意の $f \in F$ に対して $i \neq j$ となる $i, j \in \Omega_n$ が存在して

$$f = e_{X_i} + e_{X_j}.$$

ここで $X_k \subset I_k$, $|X_k| = 2$ $(k = i, j)$.

Proof. $f \in F$ とする. $|\mathrm{supp}(f) \cap I_i|$ が奇数となる $i \in \Omega_n$ が存在すると仮定する. $|\{f \in F \mid \mathrm{supp}(f) \cap I_i \neq \emptyset\}| \leq 4$ であるから $\mathrm{supp}(f') \cap I_i = \emptyset$ を満たす $f' \in F$ が存在する. $f + f' \in \mathcal{D} \subset (D_4^n)^\perp$ であるが $(f + f', e_{I_i}) = 1$ となり矛盾. したがって任意の $i \in \Omega_n$ に対して $|\mathrm{supp}(f) \cap I_i|$ は偶数. $F \cap F_0 = \emptyset$ より $|\mathrm{supp}(f) \cap I_i| \in \{0, 2\}$. □

3.3.1 Length が奇数の場合

Lemma 30. $n \geq 5$ を奇数とする. $\mathcal{D}$ を length $4n$ の self-orthogonal binary code とし, F_0 を Type B の frame として持つとする. F を $\mathcal{D}$ の Type B の frame で $F \cap F_0 = \emptyset$ とすると $|F \cap F_0| < |\sigma(F) \cap F_0|$ を満たす $\sigma \in \mathrm{Aut}(\mathcal{D})$ が存在する.

Proof. $f \in F$ とする. Lemma 29 より $i \neq j$ となる $i, j \in \Omega_n$ が存在して $f = e_{X_i} + e_{X_j}$. ここで $X_k \subset I_k$, $|X_k| = 2$ $(k = i, j)$. n が奇数であることから $\sum_{g \in F \setminus \{f\}} g \in \mathcal{D}$. また $\sum_{k \in \Omega_n \setminus \{j\}} e_{I_k} \in \mathcal{D}$.

$$\begin{aligned} e_{X_i} + e_{I_j \setminus X_j} &= \sum_{k \in \Omega_n} e_{I_k} + f + \sum_{k \in \Omega_n} e_{I_k} + e_{I_j} \\ &= \sum_{g \in F \setminus \{f\}} g + \sum_{k \in \Omega_n \setminus \{j\}} e_{I_k} \\ &\in \mathcal{D}. \end{aligned}$$

$\{s, t\} = X_i, \{u, r\} = I_j \setminus X_j$ とし, $\sigma = (s, u)(t, r)$ とする.

$$\sigma(f) = e_{I_j}.$$

Lemma 24 より $\sigma \in \mathrm{Aut}(\mathcal{D})$. □

3.3.2 Length が偶数の場合の証明の準備

$$F_1 = \bigcup_{i=0}^{k-1} \{e_{8i+1} + e_{8i+2} + e_{8i+5} + e_{8i+6}, e_{8i+3} + e_{8i+4} + e_{8i+7} + e_{8i+8}\}$$

とおく.

Definition 31. $i \in \Omega_{k-1} \cup \{0\}$ に対して $\varphi_{i,(0,0)}, \varphi_{i,(0,1)}, \varphi_{i,(1,0)}, \varphi_{i,(1,1)} \in S_n$ をそれぞれ

$$\begin{aligned}
\varphi_{i,(0,0)} &= (8i+1, 8i+7)(8i+2, 8i+8), \\
\varphi_{i,(0,1)} &= (8i+1, 8i+8)(8i+2, 8i+7), \\
\varphi_{i,(1,0)} &= (8i+3, 8i+5)(8i+4, 8i+6), \\
\varphi_{i,(1,1)} &= (8i+3, 8i+6)(8i+4, 8i+5).
\end{aligned}$$

によって定義する.

$$\begin{aligned}
\Phi_0 &= \{\varphi_{0,x} \mid x \in \boldsymbol{F}_2^2\}, \\
\Phi &= \{\varphi_{0,x_0} \dots \varphi_{k-1,x_{k-1}} \mid x_i \in \boldsymbol{F}_2^2, i \in \Omega_{k-1} \cup \{0\}\}
\end{aligned}$$

と定義する.

Lemma 32. 任意の $g \in \Phi$ に対して $g(F_1) = F_0$.

Proof. $i \in \Omega_{k-1} \cup \{0\}$ に対して,

$$\begin{aligned}
&\varphi_{i,(0,0)}(e_{8i+1} + e_{8i+2} + e_{8i+5} + e_{8i+6}) \\
=&\varphi_{i,(0,1)}(e_{8i+1} + e_{8i+2} + e_{8i+5} + e_{8i+6}) \\
=&\varphi_{i,(1,0)}(e_{8i+3} + e_{8i+4} + e_{8i+7} + e_{8i+8}) \\
=&\varphi_{i,(1,1)}(e_{8i+3} + e_{8i+4} + e_{8i+7} + e_{8i+8}) \\
=&e_{8i+5} + e_{8i+6} + e_{8i+7} + e_{8i+8} \\
\in&F_0.
\end{aligned}$$

$$\begin{aligned}
&\varphi_{i,(0,0)}(e_{8i+3} + e_{8i+4} + e_{8i+7} + e_{8i+8}) \\
=&\varphi_{i,(0,1)}(e_{8i+3} + e_{8i+4} + e_{8i+7} + e_{8i+8}) \\
=&\varphi_{i,(1,0)}(e_{8i+1} + e_{8i+2} + e_{8i+5} + e_{8i+6}) \\
=&\varphi_{i,(1,1)}(e_{8i+1} + e_{8i+2} + e_{8i+5} + e_{8i+6}) \\
=&e_{8i+1} + e_{8i+2} + e_{8i+3} + e_{8i+4} \\
\in&F_0.
\end{aligned}$$

$i, j \in \Omega_{k-1} \cap \{0\}$, $i \neq j$ とする. $x \in \boldsymbol{F}_2^2$ に対して,

$$\varphi_{j,x}(e_{8i+1} + e_{8i+2} + e_{8i+5} + e_{8i+6}) = e_{8i+1} + e_{8i+2} + e_{8i+5} + e_{8i+6}.$$
$$\varphi_{j,x}(e_{8i+3} + e_{8i+4} + e_{8i+7} + e_{8i+8}) = e_{8i+3} + e_{8i+4} + e_{8i+7} + e_{8i+8}.$$

□

Definition 33. $d_1 = (11000000)$, $d_2 = (00110000)$, $d_3 = (00001100)$, $d_4 = (00000011)$, $d_5 = (10101010)$ とする.

$$D = \langle d_1, d_2, d_3, d_4, d_5 \rangle.$$

$v = (v_1, \ldots, v_k) \in D^k$ とする. $j \in \Omega_k$ に対して $w_v(j) \in D^k$ を

$$w_v(j)_i = \begin{cases} v_j & (i = j), \\ 0 & (i \in \Omega_k \setminus \{j\}) \end{cases}$$

によって定義する.

$$\begin{aligned} w_v(j) \in \{d_1 + d_2, d_3 + d_4\} \text{ ならば } w_v(j) \in F_0, \\ w_v(j) \in \{d_1 + d_3, d_2 + d_4\} \text{ ならば } w_v(j) \in F_1 \end{aligned} \tag{32}$$

$D^k = \langle F_0, F_1 \rangle^\perp$ である.

Definition 34. $v \in D$ に対して $H_v = \{x \in \boldsymbol{F}_2^2 \mid \varphi_{0,x}(v) = v\}$ とする. $\chi_1 : D \to \boldsymbol{F}_2^2$ を

$$\chi_1(v) = \begin{cases} (0,0) & (H_v = \boldsymbol{F}_2^2 \text{ or } \emptyset), \\ (0,1) & (H_v = \{(0,0),(0,1)\} \text{ または } \{(1,0),(1,1)\}), \\ (1,0) & (H_v = \{(0,0),(1,0)\} \text{ または } \{(0,1),(1,1)\}), \\ (1,1) & (H_v = \{(0,0),(1,1)\} \text{ または } \{(0,1),(1,0)\}) \end{cases}$$

によって定義する. $\chi_2 : D \longrightarrow \boldsymbol{F}_2$ を

$$\chi_2(v) = \begin{cases} 0 & (\varphi_{0,(0,0)}(v) = v), \\ 1 & (\text{その他}) \end{cases}$$

によって定義する.

$$\chi_1((v_1, \ldots, v_k)) = (\chi_1(v_1), \ldots, \chi_1(v_k)),$$
$$\chi_2((v_1, \ldots, v_k)) = \sum_{i=1}^{k} \chi_2(v_i)$$

によって $\chi_1 : D^k \to \boldsymbol{F}_2^{2k}$, $\chi_2 : D^k \to \boldsymbol{F}_2$ に拡張する.

Lemma 35. χ_1, χ_2 は群の準同型写像.

Lemma 36.

$$\begin{aligned}\operatorname{Ker}\chi_1 &= \langle d_1+d_2, d_1+d_3, d_3+d_4\rangle,\\ \operatorname{Ker}\chi_2 &= \langle d_1+d_4, d_2, d_3, d_5\rangle.\end{aligned}$$

Definition 37.

$$E = \langle \{f+f' \mid f, f' \in F_0\} \cup \{f+f' \mid f, f' \in F_1\}\rangle.$$

任意の $f_0 \in F_0$ に対して $E_0 = E + f_0$, 任意の $f_1 \in F_1$ に対して $E_1 = E + f_1$ とする. E_0 と E_1 はそれぞれ f_0, f_1 に依存せず一意的に定まることに注意する.

Lemma 36 より $\operatorname{Ker}\chi_1 = \langle d_1+d_2, d_1+d_3, d_3+d_4\rangle$, $\operatorname{Ker}\chi_1 \cap (\operatorname{Ker}\chi_2 + d_1) = \{d_1+d_2, d_1+d_3, d_2+d_4, d_3+d_4\}$ である. $\Xi = \operatorname{Ker}\chi_1 \cap (\operatorname{Ker}\chi_2 + d_1)$ とおく.

Lemma 38. $v = (v_1, \ldots, v_k) \in D^k$ とする. $|\{i \in \Omega_k \mid v_i \in \Xi\}|$ が奇数となる必要十分条件は $\sum_{i\in\Omega_k, v_i\in\Xi} w_v(i) \in E_0 \cup E_1$.

Proof. $|\{i \in \Omega_k \mid v_i \in \Xi\}|$ が奇数ならば $\sum_{i\in\Omega_k, v_i\in\Xi} w_v(i) \in E_0 \cup E_1$ であることを $|\{i \in \Omega_k \mid v_i \in \Xi\}|$ に関する帰納法によって証明する. $|\{i \in \Omega_k \mid v_i \in \Xi\}| = 1$ のとき, $\{i \in \Omega_k \mid v_i \in \Xi\} = \{j\}$ とする. (32) より $\sum_{i\in\Omega_k, v_i\in\Xi} w_v(i) = w_v(j) \in F_0$ または F_1. $i \in \{0,1\}$ に対して $F_i \subset E_i$ であるから $|\{i \in \Omega_k \mid v_i \in \Xi\}| = 1$ のとき成り立つ.

$|\{i \in \Omega_k \mid v_i \in \Xi\}| \le m$ のとき $\sum_{i\in\Omega_k, v_i\in\Xi} w_v(i) \in E_0 \cup E_1$ であると仮定する. $|\{i \in \Omega_k \mid v_i \in \Xi\}| = m+2$ のとき $j \ne l$ となる $j, l \in \{i \in \Omega_k \mid v_i \in \Xi\}$ に対して, $w_v(j) + w_v(l) \in E \cup (E_0 + E_1)$ である. また, 帰納法の仮定から $\sum_{i\in\Omega_k\setminus\{j,l\}, v_i\in\Xi} w_v(i) \in E_0 \cup E_1$ である. よって

$$\begin{aligned}\sum_{\substack{i\in\Omega_k\\ v_i\in\Xi}} w_v(i) &= \sum_{\substack{i\in\Omega_k\setminus\{j,l\}\\ v_i\in\Xi}} w_v(i) + w_v(j) + w_v(l)\\ &\in E_0 \cup E_1 + E \cup (E_0 + E_1)\\ &= (E_0 + E) \cup (E_1 + E) \cup (E_0 + (E_0 + E_1)) \cup (E_1 + (E_0 + E_1))\\ &= E_0 \cup E_1.\end{aligned}$$

逆に$\sum_{i\in\Omega_k,v_i\in\Xi} w_v(i)\in E_0$とする. $w_v(j)\in F_0$かつ$\sum_{i\in\Omega_k\setminus\{j\},v_i\in\Xi} w_v(i)\in E$となる$j\in\{i\in\Omega_k\mid v_i\in\Xi\}$が存在する.

$$\begin{aligned}
&\sum_{i\in\Omega_k\setminus\{j\},w_v(i)\in F_0} w_v(i)+\sum_{i\in\Omega_k\setminus\{j\},w_v(i)\in F_1} w_v(i)\\
=&\sum_{\substack{i\in\Omega_k\setminus\{j\},\\ v_i\in\{d_1+d_2,d_3+d_4\}}} w_v(i)+\sum_{\substack{i\in\Omega_k\setminus\{j\},\\ v_i\in\{d_1+d_3,d_2+d_4\}}} w_v(i)\\
=&\sum_{i\in\Omega_k\setminus\{j\},v_i\in\Xi} w_v(i)\\
\in&E. \qquad (33)
\end{aligned}$$

$$\begin{aligned}
&|\{i\in\Omega_k\setminus\{j\}\mid v_i\in\Xi\}|\\
=&|\{i\in\Omega_k\setminus\{j\}\mid w_v(i)\in F_0\}|\\
+&|\{i\in\Omega_k\setminus\{j\}\mid w_v(i)\in F_1\}|\\
\equiv&0 \pmod 2. \qquad ((33)\text{より})
\end{aligned}$$

よって$|\{i\in\Omega_k\mid v_i\in\Xi\}|$は奇数である. □

Lemma 39. $v\in D^k$とすると

$$\sum_{\substack{i\in\Omega_k\\ v_i\in\operatorname{Ker}\chi_1\setminus\Xi}} w_v(i)\in E\cup(E_0+E_1).$$

Proof. Lemma 36より$\operatorname{Ker}\chi_1\setminus\Xi=\langle d_1+d_4,d_2+d_3\rangle$である. $v_i\in\{d_1+d_4,d_2+d_3\}$となる$i\in\Omega_k$に対して$w_v(i)\in E_0+E_1$であるから

$$\sum_{\substack{i\in\Omega_k\\ v_i\in\{d_1+d_4,d_2+d_3\}}} w_v(i)\in E\cup(E_0+E_1). \qquad (34)$$

また, $v_i\in\langle d_1+d_2+d_3+d_4\rangle$となる$i\in\Omega_k$に対して$w_v(i)\in E$.

$$\sum_{\substack{i\in\Omega_k\\ v_i\in\langle d_1+d_2+d_3+d_4\rangle}} w_v(i)\in E. \qquad (35)$$

$$
\begin{aligned}
&\sum_{\substack{i\in\Omega_k\\ v_i\in\operatorname{Ker}\chi_1\setminus\Xi}} w_v(i)\\
=&\sum_{\substack{i\in\Omega_k\\ v_i\in\{d_1+d_4,d_2+d_3\}}} w_v(i)+\sum_{\substack{i\in\Omega_k\\ v_i\in\langle d_1+d_2+d_3+d_4\rangle}} w_v(i)\\
\in&E\cup(E_0+E_1)+E && ((34),(35)\text{ より})\\
=&E\cup(E_0+E_1).
\end{aligned}
$$

□

Lemma 40. $v\in D^k$ とする. $\chi_1(v)=0$ かつ $\chi_2(v)=1$ となる必要十分条件は $v\in E_0\cup E_1$.

Proof. $v=(v_1,\dots,v_k)$ とする.

$$
\begin{aligned}
&\chi_1(v)=0\text{ かつ}\chi_2(v)=1\\
\Longleftrightarrow&\forall i\in\Omega_k, v_i\in\operatorname{Ker}\chi_1\text{かつ}\\
&|\{i\in\Omega_k\mid v_i\in\Xi\}|\text{ は奇数}\\
\Longleftrightarrow&\forall i\in\Omega_k, v_i\in\operatorname{Ker}\chi_1\text{かつ}\\
&\sum_{i\in\Omega_k, v_i\in\Xi} w_v(i)\in E_0\cup E_1 && (\text{Lemma 38 より})\\
\Longleftrightarrow&v\in E\cup(E_0+E_1)+E_0\cup E_1 && (\text{Lemma 39 より})\\
\Longleftrightarrow&v\in E_0\cup E_1.
\end{aligned}
$$

□

$v\in D$ とする.

$$\{v+g(v)\mid g\in\Phi_0\}\subset\{(00000000), d_1+d_4, d_2+d_3\}.$$

$x\in\langle d_1+d_4, d_2+d_3\rangle$ の $\langle d_1+d_2+d_3+d_4\rangle$ に関する剰余類を $[x]$ と書く.

Lemma 41. $v\in D$ とする.

$$[v+\varphi_{0,x}(v)]=\begin{cases}[(00000000)] & ((\chi_1(v),x)=\chi_2(v)),\\ [d_1+d_4] & (\text{otherwise}).\end{cases}$$

Proof. $x \in \boldsymbol{F}_2^2$ とする.

$$\varphi_{0,x}(v) = v \iff (\chi_1(v), x) = \chi_2(v).$$

□

Lemma 42. $v \in D^k$ とする.

$$\begin{aligned}&\{g \in \Phi \mid v + g(v) \in E\}\\ =&\{\varphi_{0,x_0} \dots \varphi_{k-1,x_{k-1}} \mid (x_0, \dots, x_{k-1}) \in \boldsymbol{F}_2^{2k}, (\chi_1(v), (x_0, \dots, x_{k-1})) = \chi_2(v)\}.\end{aligned}$$

Proof. $v = (v_1, \dots, v_k)$ とする. $(x_0, \dots, x_{k-1}) \in \boldsymbol{F}_2^{2k}$ に対して,

$$\begin{aligned}&(\chi_1(v), (x_0, \dots, x_{k-1}))\\ =&\sum_{i=1}^{k} (\chi_1(v_i), x_{i-1})\\ =&\sum_{i=1}^{k} \chi_2(v_i) + \sum_{i \in \Omega_k, (\chi_1(v_i), x_{i-1}) \neq \chi_2(v_i)} (\chi_1(v_i), x_{i-1})\\ =&\sum_{i=1}^{k} \chi_2(v_i)\\ &+|\{i \in \Omega_k \mid [v_i + \varphi_{i-1,x_{i-1}}(v_i)] = [d_1 + d_4]\}| \bmod 2 \quad \text{(Lemma 41 より)}\\ =&\chi_2(v)\\ &+|\{i \in \Omega_k \mid [v_i + \varphi_{i-1,x_{i-1}}(v_i)] = [d_1 + d_4]\}| \bmod 2. \qquad (36)\end{aligned}$$

$$\begin{aligned}&v + \varphi_{1,x_0} \dots \varphi_{k,x_{k-1}}(v) \in E\\ \iff &|\{i \in \Omega_k \mid [v_i + \varphi_{i-1,x_{i-1}}(v_i)] = [d_1 + d_4]\}| \text{ は偶数}\\ \iff &(\chi_1(v), (x_0, \dots, x_{k-1})) = \chi_2(v). \qquad \text{((36) より)}\end{aligned}$$

□

Lemma 43. $\mathcal{D}$ を F_0 を Type B の frame として持つ length $4n$ の self-orthogonal binary code とする. F_1 を $\mathcal{D}$ の Type B の frame とすると $i \in \{0, 1\}$ に対して $E_i \cap \mathcal{D} = \emptyset$.

Proof. F_i が Type B であることから $F_i \cap \mathcal{D} = \emptyset$ である. $E \subset \mathcal{D}$ より $E_i \cap \mathcal{D} = \emptyset$. □

Lemma 44. $\mathcal{D}$ を F_0 を Type B の frame として持つ length $4n$ の self-orthogonal binary code とする． F_1 を $\mathcal{D}$ の Type B の frame とすると $\bigcap_{c\in\mathcal{D}}\{g \in \Phi \mid c + g(c) \in E\} \neq \emptyset$.

Proof. $\mathcal{D} = \langle c_1, \ldots, c_l\rangle$ とする．$i \in \Omega_l$ に対して $c_i = (c_{i,1}, \ldots, c_{i,k})$ とする．ここで $c_{i,j} \in D$ $(j \in \Omega_k)$. $l \times 2k$ 行列 X を $X_{ij} = \chi_1(c_{i,j})$ によって定義する．また, $l \times (2k + 1)$ 行列 Y を

$$Y_{ij} = \begin{cases} X_{ij} & (j \in \Omega_k) \\ \chi_2(c_i) & (j = k + 1) \end{cases}$$

によって定義する．Lemma 43 より任意の $c \in \mathcal{D}$ に対して $c \notin E_0$ かつ $c \notin E_1$ が成り立つ.

$$\begin{aligned}
&\forall c \in \mathcal{D}, c \notin E_0 \text{かつ } c \notin E_1 \\
\Longleftrightarrow &\forall c \in \mathcal{D}, \\
&\chi_1(c) \neq 0 \text{ または} \chi_2(c) = 0 && \text{(Lemma 40 より)} \\
\Longleftrightarrow &\forall (y_1, \ldots, y_l) \in \boldsymbol{F}_2^l, \\
&\chi_1(\sum_{i=1}^{l} y_i c_i) \neq 0 \text{ または} \chi_2(\sum_{i=1}^{l} y_i c_i) = 0 \\
\Longleftrightarrow &\forall (y_1, \ldots, y_l) \in \boldsymbol{F}_2^l, \\
&\sum_{i=1}^{l} y_i \chi_1(c_i) \neq 0 \text{ または} \sum_{i=1}^{l} y_i \chi_2(c_i) = 0 \\
\Longleftrightarrow &\forall y \in \boldsymbol{F}_2^l, \\
&yX \neq 0 \text{ または } y(\chi_2(c_1), \ldots, \chi_2(c_l))^T = 0 \\
\Longleftrightarrow &\forall y \in \boldsymbol{F}_2^l, \\
&yX = 0 \text{ ならば } y(\chi_2(c_1), \ldots, \chi_2(c_l))^T = 0 \\
\Longleftrightarrow &\forall y \in \boldsymbol{F}_2^l, yX = 0 \text{ ならば } yY = 0 \\
\Longleftrightarrow &\operatorname{rank}(X) = \operatorname{rank}(Y) \\
\Longleftrightarrow &\exists (x_1, \ldots, x_k) \in \boldsymbol{F}_2^{2k}, \\
&\forall i \in \Omega_l, (\chi_1(c_i), (x_1, \ldots, x_k)) = \chi_2(c_i)
\end{aligned}$$

$$\begin{aligned}
&\Longleftrightarrow \exists (x_1, \ldots, x_k) \in \boldsymbol{F}_2^{2k}, \\
&\quad \forall c \in \mathcal{D}, (\chi_1(c), (x_1, \ldots, x_k)) = \chi_2(c) \\
&\Longleftrightarrow \bigcap_{c \in \mathcal{D}} \{g \in \Phi \mid c + g(c) \in E\} \neq \emptyset. \qquad \text{(Lemma 42 より)}
\end{aligned}$$

□

Lemma 45. $\mathcal{D}$ を F_0 を Type B の frame として持つ length $4n$ の self-orthogonal binary code とする． F_1 を $\mathcal{D}$ の Type B の frame とすると $g \in \mathrm{Aut}(\mathcal{D})$ が存在して $g(F_1) = F_0$.

Proof. Lemma 44 よりある $g \in \Phi$ が存在して任意の $c \in \mathcal{D}$ に対して $g(c) \in E + c \subset \mathcal{D}$. したがって $g \in \mathrm{Aut}(\mathcal{D})$. Lemma 32 より $g(F_1) = F_0$. □

3.3.3 Length が偶数の場合

$n \geq 5$ を偶数とする． $n = 2k$ とおく. $\mathcal{D}$ を length $4n$ の self-orthogonal binary code とし, F_0 を Type B の frame として持つとする. F を $\mathcal{D}$ の Type B の frame で $F \cap F_0 = \emptyset$ とする. $f, f' \in F$ を $f \neq f'$ とする. Lemma 29 より f, f' について以下の場合が考えられる.

(i) $|\{i \in \Omega_n \mid \mathrm{supp}(f + f') \cap I_i \neq \emptyset\}| = 2$

(ii) $|\{i \in \Omega_n \mid \mathrm{supp}(f + f') \cap I_i \neq \emptyset\}| = 3$

(iii) $|\{i \in \Omega_n \mid \mathrm{supp}(f + f') \cap I_i \neq \emptyset\}| = 4$

$N(F) = |\{\{f, f'\} \subset F \mid f, f'$は (i) を満たす $\}|$ とすると $N(F) \leq k$ であることに注意する.

Lemma 46. F を $N(F) < k$ を満たす $\mathcal{D}$ の Type B の frame で $F \cap F_0 = \emptyset$ とする. このとき (ii) を満たす元 f, f' が存在する.

Proof. 対偶を示す. F に (ii) を満たす元 f, f' が存在しないとする. Lemma 29 より任意の $g \in F$ を $g = e_{X_i} + e_{X_j}$ とおける. $\mathrm{supp}(g') \supset I_i \setminus X_i$ を満たす $g' \in F$ が存在する. g, g' は (iii) を満たさないので (i) を満たす. よって $N(F) = k$ である. □

Lemma 47. F を $N(F) < k$ を満たす $\mathcal{D}$ の Type B の frame で $F \cap F_0 = \emptyset$ とする. このとき $N(F) < N(\sigma(F))$ を満たす $\sigma \in \mathrm{Aut}(\mathcal{D})$ が存在する.

Proof. $N(F) < k$ であるから Lemma 46 より (ii) を満たす $f, f' \in F$ が存在する. $f + f' = e_{I_i} + e_{X_j} + e_{X_k}$ とする. ここで $i, j, k \in \Omega_n$ は互いに異なり, $X_l \subset I_l$, $|X_l| = 2$ $(l = j, k)$. Lemma 29 より $f = e_{X_i} + e_{X_j}$ とおける. ここで $X_i \subset I_i$.

$$e_{I_j \setminus X_j} + e_{X_k} = f + f' + e_{I_i} + e_{I_j} \in \mathcal{D}.$$

$\{s, t\} = I_j \setminus X_j$, $\{u, r\} = X_k$ とし $\sigma = (s, u)(t, r)$ とすると Lemma 24 より $\sigma \in \mathrm{Aut}(\mathcal{D})$. $\sigma(f + f') = e_{I_i} + e_{I_j}$ より $\{\sigma(f), \sigma(f')\} \in \{\{g, g'\} \subset \sigma(F) \mid g, g'$は (i) を満たす $\}$. 任意の $\{g, g'\} \in \{\{g, g'\} \subset F \setminus \{f, f'\} \mid g, g'$は (i) を満たす $\}$ に対して $\sigma(g) = g$ かつ $\sigma(g') = g'$ であるから $\mathrm{supp}(g + g') \cap (I_j \cup I_k) = \emptyset$. よって $\{g, g'\} \in \{\{g, g'\} \subset \sigma(F) \mid g, g'$は (i) を満たす $\}$. したがって $N(F) < N(\sigma(F))$. □

Lemma 48. F を $\mathcal{D}$ の Type B の frame で $F \cap F_0 = \emptyset$ とする. このとき $N(\tau(F)) = k$ を満たす $\tau \in \mathrm{Aut}(\mathcal{D})$ が存在する.

Proof. $k - N(F)$ に関する帰納法によって示す. $k - N(F) = 0$ のときは τ として単位置換 $e \in \mathrm{Aut}(\mathcal{D})$ ととればよい. $k - N(F) \leq l$ のとき命題が成り立つと仮定する. $k - N(F) = l + 1$ のとき Lemma 47 より $\sigma \in \mathrm{Aut}(\mathcal{D})$ が存在して $N(\sigma(F)) \leq l$. よって帰納法の仮定から $\tau \in \mathrm{Aut}(\mathcal{D})$ が存在して $N(\tau\sigma(F)) = k$. □

Lemma 49. F を $\mathcal{D}$ の Type B の frame で $F \cap F_0 = \emptyset$ かつ $N(F) = k$ とすると, $\tau(F) = F_1$ かつ $\tau(F_0) = F_0$ を満たす $\tau \in S_{4n}$ が存在する.

Proof. $e_{X_i} + e_{X_j} \in F$ に対して $e_{I_i \setminus X_i} + e_{I_j \setminus X_j} \in F$ が存在する. ここで $X_l \subset I_l$, $|X_l| = 2$ $(l = i, j)$. $i \in \Omega_{k-1} \cup \{0\}$ に対して $f_{i,1}, f_{i,2} \in F$ をそれぞれ

$$f_{i,1} = e_{X_{S_i}} + e_{X_{T_i}},$$
$$f_{i,2} = e_{I_{S_i} \setminus X_{S_i}} + e_{I_{T_i} \setminus X_{T_i}}$$

とすると $F = \{f_{i,1} \mid i \in \Omega_{k-1} \cup \{0\}\} \cup \{f_{i,2} \mid i \in \Omega_{k-1} \cup \{0\}\}$. $X_{S_i} = \{x_{i,1}, x_{i,2}\}$, $I_{S_i} \setminus X_{S_i} = \{x_{i,3}, x_{i,4}\}$, $X_{T_i} = \{x_{i,5}, x_{i,6}\}$, $I_{T_i} \setminus X_{T_i} = \{x_{i,7}, x_{i,8}\}$ とおく.

$$\tau = \prod_{i \in \Omega_{k-1} \cup \{0\}} \prod_{j=1}^{8} (x_{i,j}, 8i + j)$$

とすると $\tau(F) = F_1$ かつ $\tau(F_0) = F_0$ である. □

Lemma 50. $n \geq 5$を偶数とする. Fを$\mathcal{D}$のType Bのframeで$F \cap F_0 = \emptyset$とすると$\sigma \in \mathrm{Aut}(\mathcal{D})$が存在して$\sigma(F) = F_0$.

Proof. Fが$N(F) = k$とするとLemma 49より$\tau(F) = F_1$かつ$\tau(F_0) = F_0$を満たす$\tau \in S_{4n}$が存在する. $\tau(\mathcal{D})$はF_0, F_1をType Bのframeとして持つためLemma 45より$g(F_1) = F_0$を満たす$g \in \mathrm{Aut}(\tau(\mathcal{D}))$が存在する. $\sigma = \tau^{-1} g \tau$とおくと$\mathrm{Aut}(\mathcal{D}) = \tau^{-1}\mathrm{Aut}(\tau(\mathcal{D}))\tau$より$\sigma \in \mathrm{Aut}(\mathcal{D})$であり, $\sigma(F) = F_0$.

Fが$N(F) < k$を満たすとする. Lemma 48より$N(\tau(F)) = k$を満たす$\tau \in \mathrm{Aut}(\mathcal{D})$が存在する. $\tau(\mathcal{D}) = \mathcal{D}$であるから$\tau(F)$は$\mathcal{D}$のType Bのframeである. 証明の前半から$\rho\tau(F) = F_0$を満たす$\rho \in \mathrm{Aut}(\mathcal{D})$が存在する. □

3.3.4 Codeの自己同型群とType Bのframeの集合

Theorem 51. $n \geq 5$とする. $\mathcal{D}$をlength $4n$のself-orthogonal binary codeとしType Bのframeを少なくとも1つは持つとする. このとき$\mathrm{Aut}(\mathcal{D})$は全てのType Bのframeの集合上transitive.

Proof. $\mathcal{D}$はF_0をType Bのframeとして持つと仮定しても一般性を失わない. $\mathcal{F}$をType Bのframe全体の集合とする. $\mathcal{F}_1 = \{F \in \mathcal{F} \mid F \cap F_0 \neq \emptyset\}$, $\mathcal{F}_2 = \{F \in \mathcal{F} \mid F \cap F_0 = \emptyset\}$とする. $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$である. $F \in \mathcal{F} \setminus \{F_0\}$に対して$\tau \in \mathrm{Aut}(\mathcal{D})$が存在して$|F \cap F_0| < |\tau(F) \cap F_0|$であることを示す. $F \in \mathcal{F}_1$のときLemma 28より成り立つ. $F \in \mathcal{F}_2$のときnが奇数の場合はLemma 30から, nが偶数の場合はLemma 50からそれぞれ成り立つ. よってLemma 23より任意の$F \in \mathcal{F}$に対して$\sigma \in \mathrm{Aut}(\mathcal{D})$が存在して$\sigma(F) = F_0$. □

4 謝辞

2年間の間, 丁寧に指導して下さった宗政昭弘先生, 第2章の内容について発表の場を与えて下さった山形大学の原田昌晃先生, 東北大学大学院情報科学研究科の田村宏樹さんには本論文について指導をして頂きました. 心より感謝いたします。東北大学大学院情報科学研究科数学教室の諸先生方, 宗政研究室の先輩方, 本学の数学教室の大学院生の皆様にも大変お世話になりました. 感謝の意を表します.

参考文献

[1] L. E. Danielsen and M. G. Parker, On the classification of all self-dual additive codes over GF(4) of length up to 12, J. Combin. Theory Ser. A **113** (2006), no. 7, 1351–1367.

[2] G. Höhn, Self-dual codes over the Kleinian four group, *Math. Ann.* **327** (2003), 227–255

[3] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly even codes, J. Math. Soc. Japan **43** (1991), 67–87.